Open Enclave SDK Project Review 2023

As a project of the Confidential Computing Consortium (CCC) in the [Incubation](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fgithub.com%2Fconfidential-computing%2Fgovernance%2Fblob%2Fmaster%2Fproject-progression-policy.md%23incubation-stage&data=04%7C01%7CSimon.Leet%40microsoft.com%7C94a8eeba10294fcb043d08d885031766%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637405595608492265%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=W3Gg5kh3i5MGjjfkK2m7iDMFSkczl9wzmXuZQzmioGA%3D&reserved=0) stage, the [Open Enclave SDK](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fgithub.com%2Fopenenclave%2Fopenenclave&data=04%7C01%7CSimon.Leet%40microsoft.com%7C94a8eeba10294fcb043d08d885031766%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637405595608502262%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=NA8PSWNZQYb4kpV8x2d2IcVTgF%2FqenohzODPHbg7Dh0%3D&reserved=0) has published a [growth plan](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fgithub.com%2Fopenenclave%2Fopenenclave%2Fpull%2F3448%2Ffiles&data=04%7C01%7CSimon.Leet%40microsoft.com%7C94a8eeba10294fcb043d08d885031766%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637405595608502262%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=rResx77QvC0ryyQvUIgLD08dOqMHJxJeIpzs1Dd4A%2Bc%3D&reserved=0) for reaching the [Graduation](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fgithub.com%2Fconfidential-computing%2Fgovernance%2Fblob%2Fmaster%2Fproject-progression-policy.md%23graduation-stage&data=04%7C01%7CSimon.Leet%40microsoft.com%7C94a8eeba10294fcb043d08d885031766%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637405595608512254%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=EXTi%2FxOs6mC9waZj4SEyn1f1ZVdOFFXPISBOCvN5B3Y%3D&reserved=0) stage in accordance with CCC Technical Advisory Council mentorship. This report summarizes updates of the project information since its annual report a year ago.

1. Updated and additional information for the project submission template since the last annual report:

* List of project official communication channels
  + The Open Enclave SDK conducts its public communication through the [oesdk@lists.confidentialcomputing.io](mailto:oesdk@lists.confidentialcomputing.io) mailing list.
* List of 3rd party dependencies – No new dependencies
* Release methodology
  + Same as before - APT repo, nuget.org as well as on Github.

1. In terms of the progress against the growth plan:

* The OE SDK has settled into quarterly release cadence as it stabilizes towards an LTS release, currently on v0.18
  + Releases are also made when there are CVEs fixed in dependent libraries.
* Continues to be actively maintained, averaging ~3.3 commits weekly(~6 at this time last year). CVEs are mitigated in a timely manner.
* The cumulative number of contributors grew to 164 over the past year, the project has been starred ~885 times (754 times in the last annual report) and forked 334 times (286 times in the last annual report).
* The community that supports OP-TEE in Open Enclave SDK has shrunk and the OP-TEE specific code is not actively maintained.
* The committers are making progress towards the completion of [Inclusive Open Source Community Orientation.](https://training.linuxfoundation.org/training/inclusive-open-source-community-orientation-lfc102/) This is currently tracked by an [issue](https://github.com/openenclave/openenclave/issues/4319) on the repo.
* At this point, the OE SDK is not ready to request a vote from the TAC to move to the Graduation stage, and will continue to iterate on its growth plan to address the remaining requirements as follows:
  + Invite contributors from other organizations to become maintainers and members of CGC as they demonstrate good contributions via PRs and/or Issues filed and/or code/design review feedback.
  + Expand to other TEEs and other OS's by inviting contributions.
  + OE SDK has not yet published a public list of adopters (i.e. ADOPTERS.md) or advertised their logos as recommended in the project progression policy.

1. For budgeting purposes
   * The Zoom account used for public meetings is funded by CCC.
   * The OE SDK DL oesdk@lists.confidentialcomputing.io is hosted via CCC’s "groups.io" site.
   * There was a basic LF license scan done.
   * No new requests.
2. [Results of license scan:](https://lfscanning.org/reports/ccc/openenclave-2021-09-16-7e3b9beb-97a5-4f46-867e-81d9e0ad5be0.html) The scan results for the first 3 are issues in the OP-TEE related directories and since that community has shrunk, we have not been able to mitigate these findings. The OE community is adding support for OpenSSL 3.0 and there is an open PR, but further work is needed.

|  |
| --- |
| **Finding #1**  **Files:**  Openenclave/devex/vscode-extension/assets/devkit/devdata.tar.gz/devdata.tar/emu/vexpress-qemu\_armv8a/rootfs.cpio.gz/rootfs.cpio/bin/busybox  Priority: Very High  **This appears to be a compiled binary / object code file that contains GPL-2.0 content without corresponding sources. This file should be removed from the repo.**  **Mitigation**: Pull devkit out of the repo and place it on a blob store. Pull it during extension’s build process and provide documentation pointing directly to public sources for creating the devkit binary (buildroot/OP-TEE test framework).        **Finding #2**  **Files**:  openenclave/devex/vscode-extension/assets/devkit/devdata.tar.gz/devdata.tar/emu/vexpress-qemu\_armv8a/rootfs.cpio.gz/rootfs.cpio/usr/bin/strace-log-merge  Priority: High  **This file contains content under LGPL-2.1, a weak copyleft license. This file should likely be removed from the repo.**  **Mitigation**: Pull devkit out of the repo and place it on a blob store. Pull it during extension’s build process and provide documentation pointing directly to public sources for creating the devkit binary (buildroot/OP-TEE test framework).      **Finding #3**  **Files**:  openenclave/devex/vscode-extension/assets/devkit/devdata.tar.gz/devdata.tar/emu/vexpress-qemu\_armv8a/qemu-system-aarch64  openenclave/devex/vscode-extension/assets/devkit/devdata.tar.gz/devdata.tar/emu/vexpress-qemu\_armv8a/rootfs.cpio.gz/rootfs.cpio/lib/libpthread-2.28.so  openenclave/devex/vscode-extension/assets/devkit/devdata.tar.gz/devdata.tar/emu/vexpress-qemu\_armv8a/rootfs.cpio.gz/rootfs.cpio/usr/bin/strace  openenclave/devex/vscode-extension/assets/devkit/devdata.tar.gz/devdata.tar/sdk/optee/ls-ls1012grapeboard/lib/openenclave/enclave/liboelibc.a/iconv.c.o  openenclave/devex/vscode-extension/assets/devkit/devdata.tar.gz/devdata.tar/sdk/optee/vexpress-qemu\_armv8a/lib/openenclave/enclave/liboelibc.a/iconv.c.o  Priority: High  **This appears to be a compiled binary / object code file. We do not recommend including binary files in the source code repo. These files should likely be removed.**  **Mitigation**: Pull devkit out of the repo and place it on a blob store. Pull it during extension’s build process and provide documentation pointing directly to public sources for creating the devkit binary (buildroot/OP-TEE test framework).      **Finding #4**:  **Files**:  openenclave/3rdparty/openssl/include/bn\_conf.h openenclave/3rdparty/openssl/include/dso\_conf.h openenclave/3rdparty/openssl/include/opensslconf.h openenclave/devex/vscode-extension/assets/devkit/devdata.tar.gz/devdata.tar/emu/vexpress-qemu\_armv8a/rootfs.cpio.gz/rootfs.cpio/etc/ssl/misc/tsget.pl openenclave/docs/GettingStartedDocs/Contributors/SignUsingEngines.md  Priority: Medium  **This file contains content under the old (pre-3.0.0) OpenSSL license. The old OpenSSL license used to require certain statements to be included in advertising materials and redistributions. Is it possible to omit these files from the repo, or to upgrade them to versions from OpenSSL 3.0.0 or later (which are under Apache-2.0)?**  5 files (show files)  **Mitigation**: Cannot delete all files. Currently adding support for OpenSSL 3.0. Developers would need some time to adopt it. |